UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/526,206	03/04/2005	Ilan Mahalal	09669-054001	7470

22511 7590 07/31/2007

OSHA LIANG L.L.P.
1221 MCKINNEY STREET
SUITE 2800
HOUSTON, TX 77010

EXAMINER	
CHEN, SHIN HON	
ART UNIT	**PAPER NUMBER**
2131	

MAIL DATE	DELIVERY MODE
07/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/526,206	MAHALAL, ILAN	
	Examiner	Art Unit	
	Shin-Hon Chen	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 April 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 April 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-7 have been examined.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-7 are rejected under 35 U.S.C. 102(e) as being anticipated by Quick et al. WO 02/054663 (hereinafter Quick).

4. As per claim 1 and 7, Quick et al. discloses a method for calculating hashing of a message in a device (i.e. mobile unit) communicating with a smartcard(i.e, subscriber identification token)(see pg. 7, lines 26-30, pg. 8, lines 1-20), storing a same hash function in the device and the smartcard(pg 8, lines 6-20), wherein the message is divided in data blocks and comprises secret data and other public data(see pg. 8, lines 6-20), and wherein the keys are only known by the smartcard (pg. 8, lines 6-8 and lines20-26: the secure key), performing a calculation of the hash function of the keys in the smartcard (see pg. 8, lines 6-26, pg. 9, lines 6-9: perform hash function on the random number and the secure key); and performing the calculation of the hash function of all or part of other public data in the device(see pg. 9, lines 6-9, 26-28: encrypt other data with the cipher key CK).

5. As per claim 2, Quick et al. discloses wherein if secret data is followed by other public data in the message, the smart card starts the calculation of the hash function of all blocks that include secret data and then sends a corresponding intermediate result to the device that continues the calculation of the hash function by using the intermediate result and other public data(see pg. 8, lines 6-26, pg. 9, lines 6-15).

6. As per claim 3, Quick et al. discloses if the hash function hashes the message block by block, and if a block of the message includes a part including secret data and another part including other public data, the smartcard performs the calculation of the hash function of this block(pg. 8, lines 6-26, pg. 9, lines 6-9).

7. As per claim 4, Quick et al. discloses wherein if public data is followed by secret data, the device starts performing the calculation of the hash function of public data and then sends the corresponding intermediate result and remaining part of the last hash block to the smartcard(see pg.. 8; lines 6-26) that continues to perform the calculation of the hash function internally by using the intermediate results, the remaining part of last hash block and secret data(see col. 8, lines 6-26, pg. 11, lines 8-14).

8. As per claim 5, Quick et al. discloses a communication device(220) configured to be coupled to a smart card(230)(see fig. 2, pg. 2), the device and the smart card storing a same hash function(see pg. 8, lines 6-26, pg. 9, .lines 6-9), a message including data blocks including secret

data and other public data, wherein secret data is only known by the smart card, wherein the communication device includes a program for performing, a hashing step in which all or part of the other public data is hashed in the communication device, and a requesting step in which, the communication device requests the smart card to perform the hash function of the secret data(see pg. 8, 6-26).

9. As per claim 6, Quick et al. disclose a smartcard coupled to a communication device(fig. 2, pg 2), the communication device and the smartcard storing a same hash function, wherein a message includes data blocks including secret data and other public data(see pg. 8, lines 20-26), wherein secret data is only known by the smartcard, wherein the smartcard includes a program for performing(see pg. 8, lines 6-9), a hashing step in which all or part of the other public data is shed in the communication device, and a requesting step in which, the communication-device requests the smartcard to perform the hash function of the secret data(see pg. 8, lines 20-26, pg. 9, lines 6-9).

Response to Arguments

10. Applicant's arguments filed on 4/18/07 have been fully considered but they are not persuasive.

Regarding applicant's remarks, applicant argues that the secret data disclosed by Quick does not secure secret data stored in the smart card. The applicant has mistaken that the secret

data to be CK and IK. However, the examiner has referred to the Secure Key as the secret data stored on the smart card, which is not output outside (Quick: page 8 lines 20-26).

On the other hand, applicant argues that the prior art of record does not disclose requesting step and hashing step. However, Quick discloses that the random number is transmitted from the mobile device to the smartcard to request CK and IK and CK and IK are generated based on performing hash function on random number and the secure key (Quick: page 8 lines 20-26).

Lastly, applicant argues that the prior art does not disclose program on smart card to perform hashing on request from communication device. However, as stated in the previous paragraph, Quick discloses that the smartcard is capable of receiving random number/request from the mobile device and generate CK and IK based on the information received using the secure key and hash function stored on the smartcard (Quick: page 8 lines 20-26). Therefore, applicant's argument is respectfully traversed.

Conclusion

11. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (571) 272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shin-Hon Chen
Examiner
Art Unit 2131

SC

CHRISTOPHER REVAK
PRIMARY EXAMINER